A LA MESA DEL CONGRESO DE LOS DIPUTADOS

El Grupo Parlamentario Popular en el Congreso, al amparo de lo establecido en el artículo 193 y siguientes del vigente Reglamento del Congreso de los Diputados, presenta la siguiente **Proposición no de Ley para proteger la identidad digital de los usuarios e impedir la impunidad del anonimato en Internet**, para su debate en **Pleno**

Madrid, 26 de diciembre de 2017

Fdo. Rafael HERNANDO FRAILE
PORTAVOZ

TGE

EXPOSICIÓN DE MOTIVOS

Cada día, millones de personas dejan su rastro en Internet a través de las redes sociales, foros, compras on-line, acceso a aplicaciones móviles, gestión de banca, registros, formularios, etc. Esta actividad genera una información constante no solo de los gustos, aficiones, preferencias y actividades sino de los rasgos que nos identifican y definen como personas, en lo que se ha denominado "identidad digital" o "identidad 2.0".

Sin embargo, llama la atención la escasa importancia que se le ha concedido hasta el momento a la protección de la identidad digital o electrónica en la red, a la huella digital con la que nos identificamos y accedemos a los servicios de Internet. Por el contrario, los cibercriminales se han percatado del negocio que supone suplantar la identidad digital de una persona u organización, así como crear perfiles falsos en las redes sociales para cometer delitos. Con razón, Stefan Gross-Selbeck, presidente de la red social para profesionales Xing, manifestó que "los datos personales son el petróleo del siglo XXI".

Este tema ha cobrado especial relevancia en España debido a que muchas personas han sufrido acoso en la red o sus cuentas en redes sociales o en servicios de Internet, y han sido suplantadas por terceros con intenciones maliciosas. Y esto preocupa tanto a los expertos como a las empresas proveedoras de servicios de redes sociales. Estas últimas ya han empezado a tomar medidas: Twitter ha creado las llamadas 'cuentas verificadas' y Facebook exige que se utilice el nombre real para constituir un perfil.

En la creación de perfiles en redes sociales principalmente, pero también en otros servicios disponibles a través de Internet, las condiciones de servicio suelen requerir de los usuarios la utilización de su identidad administrativa real para la creación de una cuenta. No obstante, en un volumen no cuantificado de casos los usuarios utilizan un pseudónimo o alias para establecer un perfil en redes sociales. A menudo incluso un mismo usuario gestiona varios perfiles en redes

sociales con distintos alias. La utilización de pseudónimos para crear perfiles en redes sociales es una práctica común que no necesariamente está vinculada a actividades maliciosas; no obstante, puede ser una fuente originaria de inseguridad jurídica en los intercambios interpersonales o entre personas y servicios a través de Internet.

Detrás de cada pseudónimo existe siempre una identidad administrativa que es la llamada a responder penalmente si se comete un delito haciendo uso de cualquier servicio de Internet con ese pseudónimo (entre otros, amenazas de muerte, difamaciones, injurias, usurpación de perfiles o, suplantación de identidad) y las Fuerzas de Seguridad y la Administración de Justicia, con la colaboración de las empresas proveedoras de servicios principalmente en las redes sociales, son las encargadas de investigar e identificar al autor o autores de dicho delito. En las investigaciones por presuntas prácticas delictivas a través de servicios de Internet, órdenes judiciales pueden requerir a las empresas de telecomunicaciones que gestionan las líneas de transmisión de datos o a las empresas que proporcionan servicios a través de Internet que proporcionen todas la información que tengan en su poder vinculada al pseudónimo sospechoso de cometer la acción delictiva, ya sean datos de conexión como la dirección IP o cualquier otro dato identificativo.

El marco legislativo considera a Internet como un lugar donde la libertad de expresión debe manifestarse con responsabilidad y bajo “el respeto al derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia”, tal como lo indica el artículo 20.4 de la Constitución Española; un espacio donde no tenga cabida la impunidad ante un delito tipificado en las leyes.

Respecto al uso fraudulento de los datos identificativos de los usuarios en servicios de Internet, las empresas y los usuarios particulares deben ser conscientes de los riesgos en los que pueden incurrir si no manejan bien la información, la privacidad y la seguridad; y de la importancia de disponer de unos

sistemas fiables de protección y gestión de la identidad digital, mediante tecnología criptográfica, para protegerse de posibles riesgos y amenazas (fraude on-line, acoso en la red, robo de información personal) que hagan peligrar su identidad digital.

La Comisión Europea se esfuerza por proteger este gran tsunami de datos privados que circulan a través de servicios y localizaciones conectadas a Internet y que se alojan peligrosamente en todo tipo de soportes digitales. Sin embargo, los expertos dudan de la eficacia de las leyes puesto que, a menudo, la tecnología se desarrolla a mayor velocidad que las normas.

Hasta hace unos años no era necesario identificarse para obtener una tarjeta prepago de un teléfono móvil; hoy, todos los puntos de venta de tarjetas prepago para telefonía móvil obligan a identificarse a través del DNI, lo que ha permitido reducir la comisión de delitos amparados en el anonimato a través de la telefonía. Por ello, debemos ir dando pasos similares para aumentar y proteger la identidad digital en la red. Esto reducirá los riesgos, aumentará la seguridad y mejorará la confianza de los usuarios en Internet a la hora de realizar transacciones y hacer uso de las redes sociales.

Al respecto, en el marco normativo español sobre la protección de datos, debemos destacar el artículo 18.4 de la Constitución española de 1978, por el que "la ley obliga a los poderes públicos a limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos", y la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal.

Por su parte, la Agencia Española de Protección de Datos, ante la preocupación por el uso de los datos digitales por menores, presentó en octubre nuevos e interesantes recursos de ayuda orientados a centros docentes y familias para fomentar la privacidad y la protección de datos en Internet.

Además de la utilización de pseudónimos en la creación de perfiles en redes sociales o en cuantas conectadas a Internet, usuarios con intenciones maliciosas o al margen de ley utilizan otros mecanismos adicionales para incrementar su anonimato en el tráfico de Internet, minimizando o directamente impidiendo que haya ningún dato que pueda servir a Fuerzas de Seguridad o a la Administración de Justicia para determinar la identidad administrativa de un individuo que hay incurrido en un presunto ilícito penal a través de un pseudónimo. Estos mecanismos adicionales son tecnologías que o bien directamente impiden la circulación de datos de identificación personal o bien bloquean, disfrazan, ocultan o cifran esos datos para que no puedan ser accedidos ni analizados ni por Fuerzas de Seguridad ni por los propios proveedores de infraestructura de red o de servicios como las redes sociales u otros en Internet. Tipos de tecnologías para el incremento del anonimato personal en el tráfico de Internet son las redes privadas virtuales (VPN), la red Tor o el cifrado de contenidos punto a punto. Con las tecnologías disponibles, un individuo puede fácilmente constituirse un perfil en cualquiera de las redes sociales habituales (pongamos por caso Twitter), sin que ni el proveedor de infraestructura de red ni el proveedor de servicio de la red social conozcan en ningún momento la dirección IP del dispositivo o dispositivos con que ese individuo se conecta al servicio de Internet; si ese individuo, operando con un pseudónimo, cometiera una acción que fuera penalmente calificable como amenaza, ninguno de los proveedores de infraestructuras o servicios podría aportar datos identificativos fiables de tal sujeto si utilizara con rigor las tecnologías de anonimato comúnmente disponibles en la actualidad para cualquier usuario.

Todos hemos conocido casos en los que el anonimato ha servido de estímulo para cometer algunos delitos en las redes, como la suplantación de identidad o el acoso a algunas personas, tales como el supuesto de pederastas con niños o hacia las mujeres.

En un Estado Democrático de Derecho la libertad de expresión no puede ser confundida con el anonimato, y si bien la utilización de pseudónimos, "alias" o perfiles distintos puede ser aceptado en determinados supuestos de ocio o de comunicación interpersonal sin fines maliciosos, no lo es la utilización del anonimato como escudo protector para conseguir intereses espurios, realizar ataques contra la dignidad personal de otros o cometer diversos tipo de acciones delictivas.

Así pues, parece urgente y necesario diseñar una estrategia integral y colectiva no sólo para proteger a las personas físicas y jurídicas ante el uso fraudulento de los datos de los usuarios en Internet, sino también para la protección de sus datos personales. En dicha estrategia debería contemplarse especialmente la exigencia de la total colaboración de las empresas proveedoras infraestructuras y de servicios en de Internet cuando la Administración de Justicia o las Fuerzas de Seguridad con autorización judicial estén investigando un posible delito.

Por todo ello, el Grupo Parlamentario Popular formula la siguiente,

PROPOSICIÓN NO DE LEY:

"El Congreso de los Diputados insta al Gobierno a impulsar las medidas que considere convenientes para:

1. *Determinar cuáles son los mecanismos que permitan proteger la identidad digital del usuario en determinados servicios de la red contra el uso fraudulento de sus datos personales, potenciando la implantación de esos mecanismos en la interacción de personas físicas y jurídicas en Internet.*

2. Estudiar la necesidad de elaborar un plan integral de seguridad y buenas prácticas en Internet, que incluya la formación de usuarios (particulares, empresas, centros escolares...), con el objeto de evitar las consecuencias negativas de la suplantación de identidad, el acoso en la red y otras amenazas.
3. Acabar definitivamente con la impunidad del anonimato en Internet, en caso de un posible delito, y modificar las leyes para restringir y limitar el acceso a la red a todos aquellos que las incumplan.
4. Crear protocolos de colaboración eficaces entre las empresas proveedoras de infraestructuras y servicios en Internet y la Administración de Justicia para facilitar la actuación de Jueces, Fiscales y Fuerzas de Seguridad y cumplir las resoluciones judiciales.
5. Arbitrar medidas para que los proveedores de servicio en internet requieran la identificación de los usuarios, mediante su identidad administrativa real, de forma previa a la utilización de dichos servicios.
6. Perseguir las acciones delictivas que se realizan en internet con la misma eficacia y agilidad que fuera de la red".